JOURNAL OF ALGEBRA 122, 250–259 (1989)

On Multiplier Groups of Finite Cyclic Planes

CHAT Y. HO

Department of Mathematics, University of Florida, Gainesville, Florida 32611

Communicated by Walter Feit

Received December 1, 1987

1. INTRODUCTION

A Singer group of a projective plane is a subgroup of collineations acting sharply transitively on the points of the plane. A cyclic plane is a projective plane with a cyclic Singer group. Infinite cyclic planes are non-Desarguesian [K]. On the other hand, all known finite cyclic planes are Desarguesian.

Let Π be a finite cyclic plane and let N be the normalizer of a Singer group S in the collineation group G. Then $N = S \cdot N_X$, where N_X is the stabilizer of a point X of Π. The group $M = N/S \cong N_X$ is independent of X and S. We call M the *multiplier group* of Π. The importance of M in the study of finite cyclic planes can be seen from Ott's result [O], which says that either Π is Desarguesian or $N = G$. In this paper we determine the structure of the Sylow 2-subgroup of M and study the relationship between M and Π. Hall [H-P, p. 265] proves that three divides $|M|$. A moment of thought yields that if Π is a Desarguesian plane of order p^k for some prime p, then $|M| = 3k$ (in general $3k$ divides $|M|$). We will show that the converse of this is true for some values of k. The element in $\mathrm{Aut}(S)$, which inverts every element of S, is known to be not in M ([B, p. 60] or [F, p. 133]). Therefore $|M| \leqslant |\mathrm{Aut}(S)|/2$. Using Galois theory of cyclotomic fields, we classify planes satisfying $|M| = |\mathrm{Aut}(S)|/2$ with the help of the Gaussian quadratic sum. Also we are able to give a complete answer to the case $|M| = |\mathrm{Aut}(S)|/4$. More precisely, we prove the following.

THEOREM. *Let Π be a finite cyclic plane of order n with the multiplier group M. Then the following hold.*

(1) *The Sylow 2-subgroup T of M is cyclic. If $|T| = 2^\alpha$ for some integer $\alpha \geqslant 0$, then $n = m^{2^\alpha}$ for some integer $m \geqslant 2$.*

0021-8693/89 $3.00

(2) *For $k = 3$, 5 or 2^α for some integer $\alpha \geq 0$, we have $|M| = 3k$ if and only if $n = p^k$ for some prime p.*

(3) *We have $|M| = |\mathrm{Aut}(S)|/2$ if and only if $n = 2$ or 4. Furthermore, $n = 2$ occurs if and only if $|M| =$ odd in this case.*

(4) *We have $|M| = |\mathrm{Aut}(S)|/4$ if and only if $n = 3$.*

Some remarks are in order. Statement (1) improves a result of Ostrom and Wagner on planar 2-subgroups [D, p. 173] for cyclic planes. The cases for the extreme values of $|M|$ are treated in (2) and (3). In particular, (2) gives a characterization of the order of a finite cyclic plane being a prime if and only if its multiplier group has order 3. The study of finite cyclic planes is equivalent to the study of finite cyclic groups with difference sets [HP]. The latter has a close relationship with cyclotomic fields and number theory. Statements (3) and (4) prove that a finite cyclic group with a difference set, whose multiplier group has order at least $|\mathrm{Aut}(S)|/4$, has order 7, 21, or 13. We will prove statement (i) in section (i) for $i = 1, ..., 4$.

1. Preliminaries and the Proof of (1)

In the rest of this paper, Π is a finite cyclic plane of order n. The full collineation (resp. multiplier) group of Π is G (resp. M). Let S be a Singer group of Π and let $N = N_G(S)$. For $X \subseteq G$, let $P(X)$ be the set of fixed points of X and $\mathrm{Fix}(X)$ be the fixed-points-lines substructure of X. An involution σ in G is a Baer involution if n is a square and $\mathrm{Fix}(\sigma)$ is a subplane of order $\sqrt{n}$ (a Baer subplane). Let $A = \mathrm{Aut}(S)$. An integer t is called a multiplier if the automorphism of S (which is also denoted by t) $s \to s^t$ is also a collineation of Π when we identify the points of Π with the elements of S. Our terminology in group theory is taken from [G], that of projective planes is taken from [HP], and that of difference sets is taken from [B]. For the convenience of the reader, we record the following two known results.

Theorem 1.1 (Hall [HP, p. 265]). *Any divisor of n is a multiplier.*

Lemma 1.2 (Ott [O, 1.4]). *Suppose U is a subgroup of N such that $|P(U)| \geq 1$. Then $|P(U)| = |C_S(U)|$. If $|C_S(U)| \neq 1$, then $C_S(U)$ is a Singer group of the subplane* $\mathrm{Fix}(U)$ *(here a triangle is also regarded as a subplane).*

The next lemma is an observation about cyclic groups.

Lemma 1.3. *We have $S = S_1 \times \cdots \times S_h$, where $S_1, ..., S_h$ are cyclic groups of distinct odd prime power orders. Two involutions α, β in A are equal if and only if $|C_S(\alpha)| = |C_S(\beta)|$.*

Proof. The first statement follows from the fact that $|S| = n^2 + n + 1$ is odd. The second conclusion holds because an involution in A either centralizes or inverts S_i for $i = 1, ..., h$.

Using structures of orbits of points and lines of various subgroups of N we now prove (1) in the following steps.

(1–1) *The Sylow 2-subgroups T of M is cyclic and the involution in T is Baer.*

Proof. Let σ be an involution in T. Then there exists $s \neq 1$ in S such that σ inverts s. Suppose σ is a perspectivity. Since s has odd order, the two involutions $\sigma, \sigma s$ are conjugate in $\langle \sigma, s \rangle$. Hence σs is also a perspectivity. Thus σ and σs have a common fixed point which is then fixed by $s = \sigma(\sigma s)$. But S acts sharply transitively on the points of Π. This contradiction proves that σ is not a perspectivity and so it is a Baer involution [HP, p. 91, Theorem 4.3]. By Lemma 1.2 we have $|C_S(\sigma)| = |P(\sigma)| = n + \sqrt{n} + 1$. Since this last number is independent of σ, Lemma 1.3 implies that T has at most one involution. So T is cyclic as desired.

(1–2) *If $|T| = 2^\alpha$, then $n = m^{2^b}$ for some integers $m \geqslant 2$ and $b \geqslant \alpha$.*

Proof. Let $|T| = 2^\alpha$. We use induction on α. For $\alpha = 0$, (1–2) certainly holds. The case $\alpha = 1$ follows from (1–1) as the involution in T is Baer.

Suppose $\alpha \geqslant 2$. Let $\tau \in T$ such that $\tau^2 = \sigma$. Let $\Omega = \mathrm{Fix}(\sigma)$, a Baer subplane. We will prove that τ does not induce the identity collineation on Ω. Let $P = C_S(\sigma)$ and $u = |P|$. Then $u = n + \sqrt{n} + 1$ by Lemma 1.2. So $S = P \times Q$, where $|Q| = n - \sqrt{n} + 1$ and σ inverts every element in Q. Let $Q_1 = Q\langle \sigma \rangle$. There are exactly u Q-orbits of points of Π and each such orbit has exactly one point in Ω. Since $\Omega = \mathrm{Fix}(\sigma)$, this shows that each Q-orbit of points is also a Q_1-orbit. So the Q-orbits of points coincide with the Q_1-orbits of points. Let l be a line of Ω. Then l carries $\sqrt{n} + 1$ points of Ω. Let Γ be the set of $n - \sqrt{n}$ points of l outside Ω. Thus σ acts fixed-point-freely on the points of Γ. So Γ is the union of $(n - \sqrt{n})/2$ $\langle \sigma \rangle$-orbits, each of size 2. We claim the following holds.

(A) Any two such $\langle \sigma \rangle$-orbits belong to different Q_1-orbits.

Deny this. Let $O_1, ..., O_u$ be the Q_1-orbits of points such that O_i contains k_i subsets of the said $\langle \sigma \rangle$-orbits. Thus there exists j such that $1 \leqslant j \leqslant u$ and $k_j > 1$. Counting the number of points in Γ yields $n - \sqrt{n} = \sum_{i=1}^{u} 2k_i$.

Let $L = l^{Q_1}$. For $i \in 1, ..., u$, let l_i be the number of lines in L passing through a point of O_i. Since L has the same cardinality as any Q_1-orbit of points, l_i equals to the number of points of O_i on l. In particular $l_i \geqslant 2k_i$, for $1 \leqslant i \leqslant u$. Counting $\{x \cap y \mid x \neq y \in L\}$ in two ways yields $|L|(|L| - 1) = \sum_{i=1}^{u} |O_i|(l_i)(l_i - 1)$. From $|L| = |O_i|$ and $l_i \geqslant 2k_i$ for $i = 1, ..., u$, the last

equation implies $n-\sqrt{n} \geqslant \sum_{i=1}^{u} 2k_i(2k_i-1)$. On the other hand, $k_j > 1$. So $\sum_{i=1}^{u} 2k_i(2k_i-1) > \sum_{i=1} u = n-\sqrt{n}$. Therefore we obtain $n-\sqrt{n} > n-\sqrt{n}$. This contradiction establishes (A).

We now return to prove that τ induces a non-identity collineation on Ω. Deny this. Thus τ fixes l. Since $\sigma = \tau^2$ acts fixed-point-freely on Γ, so does τ. Let Λ be a $\langle\tau\rangle$-orbit in Γ. Then Λ is the union of two $\langle\sigma\rangle$-orbits: Λ_1, Λ_2. Since τ fixes every point in Ω, τ leaves invariant each Q_1-orbit of points. Hence Λ_1 and Λ_2 belong to a common Q_1-orbit. This contradicts (A). Therefore τ induces a non-identity collineation on Ω. So the Sylow 2-subgroup of the multiplier group of Ω has order divisible by $2^{\alpha-1}$. By induction, the order $\sqrt{n}$ of Ω equals to m^2 for some integers $m \geqslant 2$ and $c \geqslant \alpha - 1$. This implies that $n = m^{2^{c+1}}$ and establishes (1–2) as $c+1 \geqslant \alpha$.

(1–3) *If* $|T| = 2^\alpha$, *then* $n = m^{2^\alpha}$ *for some integer* $m \geqslant 2$.

Proof. Without loss of generality, we may assume $\alpha \geqslant 1$. By (1–2), $n = m^{2^b}$ for some integers $m \geqslant 2$ and $b \geqslant \alpha$. By Theorem 1.1, m is a multiplier. Therefore m^3 is also a multiplier. Let $v = n^2+n+1$. Since $n^3 \equiv 1 \pmod{v}$, $(m^3)^{2^b} \equiv 1 \pmod{v}$. From $(m^3)^{2^{b-1}} < m^{(2^{b-1})\cdot 4} = m^{2^{b+1}} = n^2$, we obtain that $1, m^3, \ldots, (m^3)^{2^{b-1}}$ are all distinct modulo v. Hence the multiplier m^3 has order 2^b. This implies $|T| \geqslant 2^b$, which in turns yields $\alpha \geqslant b$. Therefore $\alpha = b$ and $n = m^{2^\alpha}$ as desired.

Statement (1) of the theorem follows from (1–1) and (1–3).

2. Proof of (2)

Notations are as in Section 1. Also let $v = n^2+n+1$. The following result is due to Gordon, Mills, and Welch [B, p. 89].

Theorem 2.1. *If* $n = p^k$ *for some non-negative integer* k *and prime* p, *then the multiplier group* M *consists of all the powers of* p *modulo* v.

Theorem 2.1 implies that if $n = p^k$ for some non-negative integer k and prime p, then M is a cyclic group of order $3k$ generated by p. In particular, this holds for $k = 3$, 5 or 2^α. We divide the rest of the proof of (2), which uses Lagrange's theorem and elementary properties of congruences of integers, into the following steps.

(2–1) *If* $|M| = 3 \cdot 2^\alpha$ *for some integer* $\alpha \geqslant 0$, *then* $n = p^{2^\alpha}$.

Proof. By (1–3), we obtain $n = m^{2^\alpha}$ for some integer $m \geqslant 2$. Hence m is also a multiplier of Π. Let p be the smallest prime dividing m. If $m = pq$ with $q \geqslant 1$, then $p^{2^{\alpha+1}} = (p^{2^\alpha})^2 < v = n^2+n+1$. Thus $1, p, \ldots, p^{2^{\alpha+1}}$ are dis-

tinct modulo v. Therefore the cyclic subgroup of M generated by the multiplier p has order bigger than or equal to $2^{\alpha+1}$. This implies $M = \langle p \rangle$ by Lagrange's theorem. Since $n \in M$, $n \equiv p^b \pmod{v}$ for some $0 \leqslant b < v$. From $1 \equiv n^3 \equiv p^{3b} \pmod{v}$, we conclude that $b = 2^\alpha$. Since n and p^{2^α} are both less than v, we obtain $n = p^{2^\alpha}$ as desired.

(2–2) *If* $|M| = 9$, *then* $n = p^3$ *or* p *for some prime* p.

Proof. Let p be the smallest prime dividing n, and let $n = pq$. We may assume $q > 1$. Then $p^4 < v$. Hence the cyclic subgroup of M generated by the multiplier p has order bigger than 5. This implies $M = \langle p \rangle$ by Lagrange's theorem. Since $n \in M$, we obtain $n \equiv p^b \pmod{v}$ for some $1 < b \leqslant 8$. From $1 \equiv n^3 \pmod{v}$, we get $b = 3$. Since n and p^3 are both less than v, so in fact $n = p^3$ as desired.

(2–3) *If* $|M| = 15$, *then* $n = p^5$ *or* p *for some prime* p.

Proof. Let $n = pq$, where p is the smallest prime dividing n. We may assume $q > 1$. If $p = q$, then $n = p^2$. However, this implies that the multiplier p^3 has order 2, which forces $|M|$ to be even. This contradiction proves that $q > p$.

Suppose $p^5 \geqslant v$. Since $v > p^2q^2$, this implies $p^3 > q^2$. Therefore the following holds.

(B) $p^2 > q$.

Assume $p^5 \equiv 1 \pmod{v}$. Then $p^5 = 1 + kv$. Since $p^5 \geqslant v$, so $k \geqslant 1$. From $p^5 < p^3q^2$, we obtain $k < p$. Now $1 + kv = p^5 \equiv 0 \pmod{p}$ implies $1 + k \equiv 0 \pmod{p}$, which forces $k = p - 1$ as $1 \leqslant k < p$. Therefore $p^5 = 1 + (p-1)v = p(1 + (p-1)(pq^2 + q))$. So $p^4 = p^2q^2 + pq(1-q) + 1 - q$. This implies $0 \equiv 1 - q \pmod{p}$. Let $1 - q = pw$ for some integer w. Substitute this back to the equation of p^4 to get $p^4 = p^2q^2 + (pq+1)pw$. Cancelling p on both sides yields $p^3 = pq^2 + (pq+1)w$, which implies that $0 \equiv w \pmod{p}$. Therefore p^2 divides $pw = 1 - q$. Thus p^2 divides $q - 1$. However, this contradicts (B). Hence $p^5 \not\equiv 1 \pmod{v}$ when $p^5 \geqslant v$.

Since $p^4 < v$, we conclude that $1, p, \ldots, p^5$ are all distinct modulo v. Therefore $M = \langle p \rangle$ by Lagrange's theoem as $|M| = 15$. Since $n \in M$, we get $n \equiv p^b \pmod{v}$ for some $0 \leqslant b < 15$. From $1 \equiv n^3 \pmod{v}$, we obtain $b = 5$. Hence $pq = n \equiv p^5 \pmod{v}$. Since $(p, q) = 1$, this implies $q \equiv p^4 \pmod{v}$. Therefore $q = p^4$ as both q and p^4 are less than v. This proves $n = pq = p^5$ as desired.

(2–4) *If* $|M| = 3k$, *where* $k = 3$ *or* 5, *then* $n = p^k$, *where* p *is a prime.*

Proof. By (2–3) and (2–4), it suffices to eliminate the case $n=p$, where p is a prime. If $n=p$, then Theorem 2.1 implies that $|M|=3$. This contradiction establishes (2–4).

Statement (2) follows from (2–1), (2–4), and the remark on Theorem 2.1.

3. Proof of (3)

Notations as in Section 1. Also $v=n^2+n+1=|S|$. Let ζ be a primitive vth root of 1 in the complex number field. We identify S with $\langle\zeta\rangle$ in $Q(\zeta)$, the cyclotomic field obtained by adjoining ζ to Q, the rationals. Next we identify $A=\mathrm{Aut}(S)$ with the Galois group of $Q(\zeta)$ over Q.

A subset of S is called a difference set of S if for any element $s\in S$ there exists exactly one pair of elements α, b in this set such that $s=\alpha^{-1}b$. By [B, p. 79, Theorem 4.1], there exists a difference set D of S which is left invariant by M. Set $\theta=\sum_{d\in D}\zeta^d$. Then θ belongs to K, the fixed subfield of M. With the help of the Gaussian quadratic sum we now prove (3) in the following three steps.

(3–1) *If $n=2$ (resp. $n=4$), then $|M|=|A|/2=3$ (resp. 6).*

Proof. Since planes of order 2 and 4 are Desarguesian, our conclusion follows from the general fact that for a Desarguesian plane of order $p^k=n$, where p is a prime, the multiplier group has order $3k$.

(3–2) *If $|M|=|A|/2$ is odd, then $n=2$.*

Proof. Denote the complex conjugation of x by $\bar{x}$. Since -1 is not a multiplier [B, p. 60], we obtain

(C) $\bar{\theta}\neq\theta$.

Let $g=\sum_{t=0}^{v-1}\zeta^{t^2}$ be the Gaussian quadratic sum. Then g is an algebraic integer in $Q(\zeta)$. Since v is odd, by Gauss [N, p. 117] we obtain the following.

(D) If $v\equiv\varepsilon \pmod 4$, where $\varepsilon=1$ or -1, then $g=\sqrt{\varepsilon v}$.

In particular $[Q(g):Q]=2$. Since M is the unique subgroup of index 2 in A under our assumption, we conclude that K is the unique subfield of $Q(\zeta)$ with degree 2 over Q by the fundamental theorem of Galois theory. Hence $K=Q(g)$. Note that the Galois group of K over Q is generated by the restriction of the complex conjugation.

Suppose $v\equiv 1 \pmod 4$. Then K is a subfield of the real numbers by (D). Since $\theta\in K$, this implies $\theta=\bar{\theta}$, which contradicts (C). Therefore $v\equiv 3 \pmod 4$ and $K=Q(\sqrt{-v})$ by (D) again. As $-v\equiv 1 \pmod 4$, the ring of

algebraic integers of K is $Z \oplus Z((-1+\sqrt{-v})/2)$ [IR, p. 189]. Hence $\theta = x + (y/2)(-1+\sqrt{-v})$ for some integers x and y. Since $\theta \neq \bar{\theta}$ by (C), $y \neq 0$. Also $\theta\bar{\theta} = (x - y/2)^2 + (y^2 v)/4$. On the other hand, from the definition of θ and the difference set D, we obtain $\theta\bar{\theta} = n$ as $\sum_{i=0}^{v-1} \zeta^i = 0$. Therefore $4n = 4\theta\bar{\theta} = (2x - y)^2 + y^2 v \geqslant v = n^2 + n + 1$ as $y \neq 0$. Since $n \geqslant 2$, this last inequality implies $n = 2$. The proof of (3–2) is now completed.

(3–3) *If* $|M| = |A|/2$, *then* $n = 2$ *or* 4.

Proof. By (3–2), we may assume that $|M|$ is even. Since -1 is not a multiplier and $|A| = 2|M|$, the elementary abelian 2-subgroup of A has order 4 by (1–1). This together with the fact that each Sylow subgroup of S is cyclic of odd prime power order implies that $S = S_1 \times S_2$ (see Lemma 1.3). Let σ be the involution of M. By (1–1), σ is a Baer involution. By Lemma 1.2, $|C_S(\sigma)| = n + \sqrt{n} + 1 \neq 1$. Thus $C_S(\sigma)$ is one of S_1, S_2. Without loss of generality we may assume that $C_S(\sigma) = S_1$. Since S_1 is cyclic of odd prime power order, $A_1 := \mathrm{Aut}(S_1)$ is cyclic. Hence the only involution of A_1 inverts S_1. However, S_1 acts sharply transitively on the points of $\mathrm{Fix}(\sigma) = \Omega$, so -1 is not a multiplier of Ω. This implies that the multiplier group R of Ω has odd order. Since the only involution in M centralizes S_1, $A_1 \neq M$. From $|A : M| = 2$, this implies that $A = A_1 M$. Hence $|A_1 : A_1 \cap M| = 2$. Hall [B, p. 83] proves that M induces by restriction a subgroup of the multiplier group of Ω. Therefore $A_1 \cap M \leqslant R$. Thus $A_1 \cap M = R$ as $A_1 > R$. This implies that $|R| = |A_1|/2$. Since $|R|$ is odd, so (3–2) implies that the order $\sqrt{n}$ of Ω equals 2. Therefore $n = 4$ as desired.

Statement (3) follows from (3–1), (3–2), and (3–3).

4. Proof of (4)

Notations are as in Section 3. The following is a general fact about cyclic groups of odd order.

Lemma 4.1. *Let* $S = S_1 \times \cdots \times S_h$, *where* S_i *is the cyclic Sylow* p_i*-subgroup of* S *and* $A_i = \mathrm{Aut}(S_i)$ *for* $i = 1, \ldots, h$. *For* $i = 1, \ldots, h$ *if* $p_i > 3$, *then there exists* $\sigma_i \in A_i$ *such that* σ_i *is of odd order and* $C_S(\sigma_i) = \prod_{j \neq i} S_j$.

We now prove (4) in the following steps.

(4–1) *If* $|M| = |A|/4$ *is odd, then* $n = 3$.

Proof. There are two cases for $T \cong A/M$ to be considered.

Case 1. $T \cong Z_2 \times Z_2$. We will prove that this case cannot occur. By the structure of $A = \mathrm{Aut}(S)$, the condition stated in case 1 implies that $S = S_1 \times S_2$. Let $p_1 < p_2$. So $3 < p_2$. By Lemma 4.1 there exists $\sigma_2 \in A_2$ of odd order such that $C_S(\sigma) = S_1$. Since σ_2 has odd orer, $\sigma_2 \in M$. By Lemma 1.2, S_1 acts as Singer group on the subplane $\Pi_2 = \mathrm{Fix}(\sigma_2)$.

Suppose $|S_1| > 3$. Then Π_2 is a proper subplane whose multiplier group M_2 contains $A_1 \cap M$. Since -1 is not a multiplier of Π_2 and $|A_1| = 2$ odd, so $|A_1| = 2|M_1|$. By (3–2), the order of Π_2 is 2. Hence $|S_1| = 7$, which forces $p_1 = |S_1| = 7$. Applying Lemma 4.1 to p_1 yields $\sigma_1 \in A_1$ such that σ_1 has odd order and $C_S(\sigma_1) = S_2$. Interchanging the indices 1 and 2 in the above argument, we obtain, as $p_2 > 3$, that $p_2 = |S_2| = 7$. This contradiction proves that $|S_1| = 3$.

Suppose $|S_2| > p_2$. Then there exists $\tau \in A_2$ of odd order such that $|S_2 : C_{S_2}(\tau)| = p_2$. Let $W = C_{S_2}(\tau)$. Thus $C_S(\tau) = S_1 \times W$ has order bigger than 3. By Lemma 1.2, $S_1 \times W$ is a Singer group on the proper subplane $\Delta = \mathrm{Fix}(\tau)$. Now $\mathrm{Aut}(S_1 \times W) = A_1 \times (A_2/\langle \tau \rangle)$, which shows that the multiplier group of Δ has odd order $(1/e)|\mathrm{Aut}(S_1 \times W)|$, where $e = 2$ or 4. Therefore the order w of Δ is 2 when $e = 2$ by (3–2) or 3 when $e = 4$ by induction. This implies that $|S_1 \times W| = 7$ or 13 according to $w = 2$ or 3. But $|S_1| = 3$. This contradiction proves that case 1 cannot occur.

Case 2. T is cyclic of order 4. This implies that S is a p-group for some prime p. First we show that $|S| = p$. Deny this. Then there exists $\sigma \in A$ of odd order such that $V = C_S(\sigma)$ has index p in S. If $|V| = 3$, then $|S| = 9 = n^2 + n + 1$, which is impossible. Hence $|V| > 3$. By Lemma 1.2, V acts as a Singer group on the proper subplane $\mathrm{Fix}(\sigma)$. Since $\mathrm{Aut}(V) = A/\langle \sigma \rangle$, we get that the multiplier group of $\mathrm{Fix}(\sigma)$ has odd order $|\mathrm{Aut}(V)|/4$. By induction, the order of $\mathrm{Fix}(\sigma)$ is 3. Hence $|V| = 13$ and so $|S| = 169$, which is impossible [B, p. 88]. Therefore $|S| = p$ as desired. Hence A is cyclic.

By [B, p. 79], M fixes a line l of Π. We claim the following holds.

(E) Any subgroup of M fixing at least four points on l is the identity subgroup.

Let $H = \langle h \rangle$ be one such subgroup. By Lemma 1.2, $\mathrm{Fix}(H)$ is a proper subplane. Since $|S| = p$ is a prime, there are p conjugates of H in $\{H^s \mid s \in S\}$. As Π has p points, the set $\{P(H^s) \mid s \in S\}$ cannot be disjoint. Thus there exists $1 \neq x \in S$ such that $P(H) \cap P(H^x) \neq \varnothing$. Therefore $h^{-1}h^x$ fixes a point. But $1 \neq [h, x] \in S$, which acts sharply transitively on the points of Π. This contradiction establishes (E).

From $|S| = p$ is a prime, we get $|A| = p - 1 = n(n+1)$. Let O be an orbit of points of M on l. Suppose $|O| > 3$. By (E), M acts fixed-point-freely on O as M is cyclic. Hence $n(n+1)/4 = |M|$ divides $|O| \leqslant n + 1$. This implies that $n \leqslant 4$. Since $n = 2$ or 4 cannot occur, we have $n = 3$ and (4–1) is

established in this case. Therefore we may assume that each M-orbit of points on l has size 3 or 1 as $|M|$ is odd. If there are two orbits of size 3, then the kernel H of the action of M on each one of these orbits coincide as M is cylic. Therefore $H=1$ by (E) and M acts fixed-point-freely on an orbit of size 3. Thus $n(n+1)/4$ divides 3, which forces $n=3$. However, this contradicts the fact there are two M-orbits of size 3 on l. Since S is a Singer group, no element of M can fix all points on l. Therefore there is exactly one M-orbit of points R of size 3 on l. If there are at least two more points on l, then (E) implies that M acts fixed-point-freely on R. Again we obtain $n=3$. But we have at least $5=|R|+2$ point on l under the present assumption. This contradiction proves that there is exactly one more point on l besides the three points in R. Therefore $n+1=4$ and $n=3$ as desired. The proof of (4–1) is now complete.

(4–2) *If* $|M|=|A|/4$, *then* $n=3$.

Proof. By (4–1), we may assume that $|M|$ is even. By (1), the involution σ in M is a Baer involution. From Lemma 1.2, $C=C_S(\sigma)$ is a Singer group on the Baer subplane $\Omega=\mathrm{Fix}(\sigma)$. Since $|S|$ is odd $S=C\times[S,\sigma]$, where $|[S,\sigma]|=n-\sqrt{n}+1$, which is prime to $|C|$. Let $X=\mathrm{Aut}(C)$ and $Y=\mathrm{Aut}([S,\sigma])$. Then $|A|=|X|\,|Y|$. Let $C=\langle\gamma\rangle\subseteq S=\langle\zeta\rangle$. Then $Q(\gamma)$ is a Galois extension subfield of $Q(\zeta)$ over Q. Hence every Galois automorphism of $Q(\gamma)$ can be extended to a Galois automorphism of $Q(\zeta)$. This shows that an odd-order automorphism of C is the restriction of an element in M as M contains all odd-order automorphism of S. Therefore all odd-order automorphisms in X belong to the multiplier group J of Ω. In the proof of (1–2) we see that for $\tau\in M$ with $\tau^2=\sigma$, the restriction of τ on Ω is not the identity collineation. From this and the fact that -1 is not a multiplier of Ω, we obtain $|J|=|X|/e$, where $e=2$ or 4. If $e=4$, then induction implies that the order $\sqrt{n}$ of Ω equals 3. Hence $n=9$. But $|M|=6\neq|A|/4$ in this case. Therefore $e=2$. By (2) we obtain $\sqrt{n}=2$ or 4. The case $n=4$ cannot occur as $|M|\neq|A|/4$. So $n=16$. Since cyclic planes of order 16 are Desarguesian [D, p. 209, 5], we obtain $|M|=3\cdot4$. But $|S|=3\cdot7\cdot13$ and so $|A|=2\cdot6\cdot12\neq4|M|$. This final contradiction establishes (4–2) and completes the proof of the theorem.

References

[B] L. D. Baumert, "Cyclic Difference Sets," Lecture Notes in Mathematics Vol. 182, Springer-Verlag, New York, 1971.

[D] P. Dembowski, "Finite Geometries," Springer-Verlag, New York, 1968.

[F] M. FRIED, The field of definition of function fields and a problem in the reducibility of polynomials in two variables, *Illinois J. Math.* **17** (1973), 128–146.
[G] D. GORENSTEIN, "Finite groups," Harper & Row, New York, 1968.
[HP] D. HUGES AND F. PIPER, "Projective Planes," Springer-Verlag, New York, 1973.
[IR] K. IRELAND AND M. ROSEN, "A Classical Introduction to Modern Number Theory," Graduate Texts in Mathematics, Springer-Verlag, New York/Berlin, 1982.
[K] H. KARZEL, Ebenen Inzidenzgruppen, *Arch. Math.* **40** (1964), 10–17.
[N] T. NAGELL, "Introduction to Number Theory," Chelsea, New York, 1964.
[O] OTT, Endliche Zyklische ebenen, *Math. Z.* **144**, 195–215.

Printed in Belgium